

Method and apparatus for encrypting radio traffic in a telecommunications network**Publication number:** JP2001500327T**Publication date:** 2001-01-09**Inventor:****Applicant:****Classification:**


- International: **G09C1/00; H04L9/08; H04Q7/32; H04Q7/38; H04L9/30; G09C1/00; H04L9/08; H04Q7/32; H04Q7/38; H04L9/28; (IPC1-7): H04L9/08; G09C1/00; H04Q7/38**

- european: H04L9/08; H04Q7/32S

Application number: JP19980512543T 19970826

Priority number(s): WO1997SE01407 19970826; US19960708796 19960909

Also published as:

 WO9810561 (A1)
EP0923827 (A1)
US5850444 (A1)
EP0923827 (A0)
EP0923827 (B1)

more >>

Report a data error he

Abstract not available for JP2001500327T

Abstract of corresponding document: **US5850444**

A generic communications network provides an encrypted communications interface between service networks and their subscribers. When communications are initiated between a subscribing communications terminal and the generic network, the terminal compares a stored network identifier associated with a stored public key, with a unique identifier broadcast by the generic network. If a match is found, the terminal generates a random secret key, encrypts the secret key with the stored public key, and transmits the encrypted secret key. The generic communications network decrypts the secret key using a private key associated with the public key. The secret key is used thereafter by the terminal and the generic network to encrypt and decrypt the ensuing radio traffic. Consequently, the network can maintain secure communications with the terminal without ever knowing the terminal's identity.

Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号
特表2001-500327
(P2001-500327A)

(43) 公表日 平成13年1月9日 (2001.1.9)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 B
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R

審査請求 未請求 予備審査請求 有 (全 32 頁)

(21) 出願番号 特願平10-512543
(86) (22) 出願日 平成9年8月26日 (1997.8.26)
(85) 翻訳文提出日 平成11年3月9日 (1999.3.9)
(86) 国際出願番号 P C T / S E 9 7 / 0 1 4 0 7
(87) 国際公開番号 W O 9 8 / 1 0 6 6 1
(87) 国際公開日 平成10年3月12日 (1998.3.12)
(31) 優先権主張番号 0 8 / 7 0 8 , 7 9 6
(32) 優先日 平成8年9月9日 (1996.9.9)
(33) 優先権主張国 米国 (US)

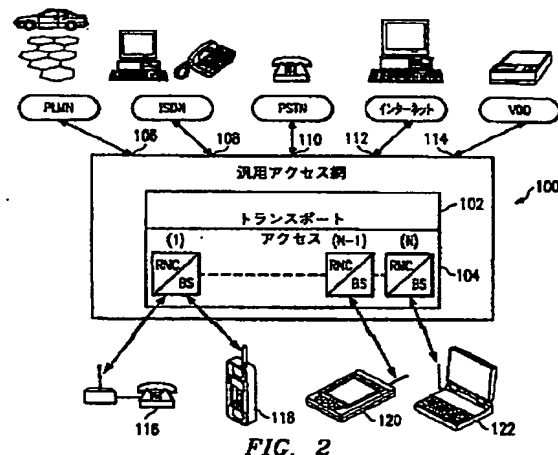
(71) 出願人 テレフオンアクチーボラゲット エル エ
ム エリクソン (パブル)
スウェーデン国エスー126 25 ストック
ホルム (番地なし)
(72) 発明者 ルネ, ヨハン
スウェーデン国 エスー181 30 リディ
ング, モーシヨンスベーク 5
(74) 代理人 弁理士 浅村 皓 (外3名)

最終頁に続く

(54) 【発明の名称】 電気通信網における無線トラフィック暗号化方法および装置

(57) 【要約】

汎用通信網 (100) はサービス網 (130, 132, 134) とそれらの加入者との間に暗号化通信インターフェイスを提供する。加入通信端末 (118) と汎用網 (100) との間で通信が開始されると、端末 (118) は保存された公開鍵に関連する保存されたネットワーク識別子を汎用網 (100) によりブロードキャストされた一意的な識別子と比較する。一致すれば、端末 (118) はランダム秘密鍵を発生し、秘密鍵を保存された公開鍵により暗号化し、暗号化された秘密鍵を送信する。汎用通信網 (100) は公開鍵に関連するプライベート鍵を使用して秘密鍵を復号する。その後、秘密鍵は端末 (118) および汎用網 (100) により後続無線トラフィックを暗号化および復号するのに使用される。したがって、網 (100) は端末のアイデンティティを知ることなく端末 (118) との安全な通信を維持することができる。



【特許請求の範囲】

1. 移動通信網と通信端末間の通信トラフィックを暗号化する方法であって、該方法は、

公開鍵および前記移動通信網に関連する第1の識別子を前記通信端末に保存するステップと、

前記通信端末に保存された前記第1の識別子を前記移動通信網から受信した第2の識別子と比較して第1の所定の結果を作り出すステップと、

前記通信端末において秘密鍵を生成するステップと、

前記通信端末において前記秘密鍵を前記保存された公開鍵により暗号化するステップと、

前記暗号化された秘密鍵を前記通信端末から送信するステップと、

を含む通信トラフィック暗号化方法。

2. 請求項1記載の方法であって、さらに、

前記移動通信網において前記暗号化された秘密鍵を受信するステップと、

前記公開鍵に関連するプライベート鍵により前記受信した暗号化された秘密鍵を復号するステップと、

前記通信トラフィックを前記秘密鍵により暗号化するステップと、

を含む方法。

3. 請求項1記載の方法であって、公開鍵を保存するステップは公開鍵を先験的に予め保存するステップを含む方法。

4. 請求項1記載の方法であって、さらに、前記通信端末から公開鍵要求を受信したら前記移動通信網から前記公開鍵を送信するステップを含む方法。

5. 請求項4記載の方法であって、前記公開鍵を送信するステップは、さらに、前記公開鍵を認証する情報を送信するステップを含む方法。

6. 請求項4記載の方法であって、さらに、前記比較ステップが第2の所定の結果を作り出したら、前記通信端末から前記要求を送信するステップを含む方法。

7. 請求項1記載の方法であって、前記暗号化された秘密鍵を受信して復号

するステップは、前記移動通信網内の無線基地局において実施される方法。

8. 請求項1記載の方法であって、前記受信した暗号化された秘密鍵を復号するステップは、前記移動通信網内の無線網コントローラにおいて実施される方法。

9. 請求項1記載の方法であって、前記移動通信網は汎用通信網を含む方法。

10. 請求項1記載の方法であって、前記通信端末は移動端末を含む方法。

11. 請求項1記載の方法であって、前記通信端末は固定端末を含む方法。

12. 請求項1記載の方法であって、前記通信端末は未確認通信端末を含む方法。

13. 請求項1記載の方法であって、前記移動通信網はセルラー電話網を含む方法。

14. 請求項1記載の方法であって、さらに、

複数のサービス網を前記移動通信網に接続するステップであって、前記通信端末のユーザは前記複数のサービス網の少なくとも1つの加入者であるステップと、

前記通信端末と前記複数のサービス網の少なくとも1つとの間に通信パスを提供するステップと、

を含む方法。

15. 請求項1記載の方法であって、前記プライベート鍵および前記公開鍵はRSAアルゴリズムにより関連づけられる方法。

16. 請求項1記載の方法であって、前記秘密鍵は対称暗号鍵を含む方法。

17. 請求項1記載の方法であって、秘密鍵を生成するステップは自然発生乱数を発生するステップを含む方法。

18. 請求項1記載の方法であって、秘密鍵を生成するステップは、
前記通信端末においてデジタル形式の受信信号を検出するステップと、
前記検出された受信信号から少なくとも1つの低位ビットを抽出するステップと、
を含む方法。

19. 請求項1記載の方法であって、秘密鍵を生成するステップは、
マイクロホンA/Dコンバータの出力において信号を検出するステップと、

前記検出された出力信号から少なくとも1つの低位ビットを抽出するステップ
と、

を含む方法。
20. 請求項1記載の方法であって、秘密鍵を生成するステップは、
音声コーデックの出力において信号を検出するステップと、

前記検出された出力信号から少なくとも1つの低位ビットを抽出するステップ
と、

を含む方法。
21. 請求項1記載の方法であって、秘密鍵を生成するステップは、
擬似乱数のシードを発生するステップと、

前記シードから擬似乱数を発生するステップと、

を含む方法。
22. 請求項1記載の方法であって、前記秘密鍵の長さは前記通信端末にお
いて予め決定される方法。
23. 請求項1記載の方法であって、前記秘密鍵はさらに複数の接続された
数字を含む方法。
24. 請求項1記載の方法であって、前記公開鍵および前記第1の識別子を
保存するステップはさらに前記公開鍵に関連する期限日付を保存するステップを
含む方法。
25. 請求項24記載の方法であって、前記通信端末は前記公開鍵の期限が
切れると前記移動通信網へ公開鍵要求を送信する方法。
26. 請求項1記載の方法であって、さらに、

前記移動通信網において前記公開鍵を変えるステップと、

前記通信端末において前記変えられた公開鍵を保存するステップと、

を含む方法。
27. 請求項26記載の方法であって、前記公開鍵を変えるステップは、さ

らに、前記変えられた公開鍵を前記移動通信網から所定期間ブロードキャストするステップを含む方法。

28. 汎用通信網と第1の通信端末との間でトラフィックを暗号化する方法

であって、該方法は、

前記汎用通信網から前記第1の通信端末を含む複数の通信端末へ公開鍵をブロードキャストするステップと、

前記第1の通信端末において秘密鍵を生成するステップと、

前記第1の通信端末において前記秘密鍵を前記公開鍵により暗号化するステップと、

前記暗号化された秘密鍵を前記第1の通信端末から送信するステップと、

前記汎用通信網において前記暗号化された秘密鍵を受信するステップと、

前記受信した暗号化された秘密鍵を前記公開鍵に関連するプライベート鍵により復号するステップと、

前記トラフィックを前記秘密鍵により暗号化するステップと、

を含む方法。

29. 請求項28記載の方法であって、ブロードキャストするステップは、さらに、

前記公開鍵を無線網コントローラから前記汎用通信網内の少なくとも1つの基地局へ転送するステップと、

前記公開鍵を前記少なくとも1つの基地局から送信するステップと、

を含む方法。

30. 請求項28記載の方法であって、ブロードキャストするステップは、前記公開鍵を前記汎用通信網内の複数の基地局から送信するステップを含む方法。

31. 請求項28記載の方法であって、前記第1の通信端末は未確認通信端末を含む方法。

32. 請求項28記載の方法であって、前記公開鍵をブロードキャストするステップは、さらに、前記公開鍵を認証する情報をブロードキャストするステッ

ブを含む方法。

33. 請求項28記載の方法であって、前記公開鍵をブロードキャストするステップは、さらに、前記公開鍵を認証する情報を要求に応じて送信するステップを含む方法。

34. 移動通信網と通信端末間の通信トラフィックを暗号化する方法であっ

て、該方法は、

ディフィーヘルマン指数鍵交換アルゴリズムに関連する2つの数字および前記移動通信網に関連する第1の識別子を前記通信端末において保存するステップと

、

前記通信端末に保存された前記第1の識別子を前記移動通信網から受信した第2の識別子と比較して第1の所定の結果を作り出すステップと、

前記通信端末において第1の乱数を発生するステップと、

前記移動通信網において第2の乱数を発生するステップと、

前記第1および第2の乱数を前記ディフィーヘルマン指数鍵交換アルゴリズムへの入力として使用して、前記通信端末および前記移動通信網により秘密鍵として使用される第3の数字を発生するステップと、

を含む通信トラフィック暗号化方法。

35. 請求項34記載の方法であって、2つの数字を保存するステップは前記2つの数字を先験的に予め保存するステップを含む方法。

36. 請求項34記載の方法であって、さらに、前記通信端末から前記2つの数字に対する要求を受けたら前記移動通信網から前記2つの数字を送信するステップを含む方法。

37. 請求項36記載の方法であって、さらに、前記比較ステップが第2の所定結果を生じたら前記通信端末から前記要求を送信するステップを含む方法。

38. 請求項34記載の方法であって、前記2つの数字および前記第1の識別子を保存するステップは、さらに、前記2つの数字に関連する期限日付を保存するステップを含む方法。

39. 請求項38記載の方法であって、前記2つの数字の期限が切れると、

前記通信端末は前記ディフィーヘルマン指数鍵交換アルゴリズムに関連する2つの新しい数字に対する要求を送信する方法。

40. 請求項34記載の方法であって、さらに、

前記移動通信網においてディフィーヘルマン指数鍵交換アルゴリズムに関連する前記2つの数字を変えるステップと、前記通信端末において前記変えられた2つの数字を保存するステップと、を含む方法。

41. 請求項40記載の方法であって、前記2つの数字を変えるステップは、

さらに、前記変えられた2つの数字を前記移動通信網から所定期間ブロードキャストするステップを含む方法。

42. 汎用通信網と第1の通信端末間のトラフィックを暗号化する方法であって、該方法は、

指数鍵交換アルゴリズムに関連する2つの数字を前記汎用通信網から前記第1の通信端末を含む複数の通信端末へブロードキャストするステップと、

前記第1の通信端末において第1の乱数を発生するステップと、

前記汎用通信網において第2の乱数を発生するステップと、

前記第1および第2の乱数を前記指数鍵交換アルゴリズムへの入力として使用して、前記第1の通信端末および前記汎用通信網により秘密鍵として使用される第3の数字を発生するステップと、

前記トラフィックを前記秘密鍵により暗号化するステップと、
を含む方法。

43. 汎用通信網と通信端末間のトラフィックを暗号化する方法に使用するシステムであって、該システムは、

前記汎用通信網内に含まれるアクセス網と、

前記通信端末に接続されかつ前記アクセス網と関連づけられて、前記汎用通信網に関連する公開鍵を保存し、秘密鍵を生成し、前記秘密鍵を前記保存された公開暗号鍵により暗号化し、前記暗号化された秘密鍵を前記汎用通信網へ送信するアクセス網手段と、

を含むシステム。

44. 汎用通信網と通信端末間のトラフィックを暗号化するシステムであって、該システムは、

プライベート暗号鍵を保存し、公開暗号鍵を配送し、暗号化された秘密セッション鍵を復号する第1のネットワーク手段と、

前記第1のネットワーク手段に接続されて前記配送された公開暗号鍵をブロードキャストする第2のネットワーク手段であって、前記第1および第2のネットワーク手段は前記汎用通信網のアクセス網と関連づけられている前記第2のネットワーク手段と、

前記通信端末に接続されかつ前記汎用通信網の前記アクセス網と関連づけられて、前記ブロードキャストされた公開暗号鍵を受信し、秘密鍵を生成し、前記秘密鍵を前記受信した公開暗号鍵により暗号化し、前記暗号化した秘密鍵を前記汎用通信網へ送信するアクセス網手段と、

を含むシステム。

【発明の詳細な説明】**電気通信網における無線トラフィック暗号化方法および装置****発明の背景****発明の技術分野**

本発明は一般的にワイヤレス無線通信の分野に関し、特に、端末と移動無線網間の無線トラフィックの暗号化方法および装置に関する。

関連技術の説明

電気通信網におけるモビリティおよび融通性を高める必要性から、ネットワークはより大きい地理的エリアをカバーしてより広範な電気通信サービスを加入者へ提供する必要がある。これらの電気通信サービスにはテレサービスおよびベアラサービスが含まれる。テレサービスは別の加入者（例えば、端末、等）と通信を行う加入者に必要なハードウェアおよびソフトウェアを提供する。ベアラサービスはネットワークとのインターフェイスを提供する2つのアクセスポイント（例えば、ポート）間で適切な信号を送信するのに必要な容量を提供する。電気通信サービスは、例えば、公衆陸上移動電気通信網（PLMN）、公衆交換電話網（PSTN）、統合デジタル通信サービス（ISDN）、いわゆる“インターネット”アクセス網、ビデオオンデマンド（VOD）網、その他適切なサービス網、等のいくつかのサービス網により加入者へ提供される。

モビリティおよび融通性を高める必要性に応じて、新しい移動無線電気通信網が開発されており、それはサービス網加入者をその地理的位置に無関係にそのサービス網に接続できる汎用（generic）インターフェイスを有している。この汎用アクセス網は“Generic Access Network”（GAN）といわれる。主として端末とGANとの間の通信トラフィックの暗号化に関係する本発明をより容易に理解するために、次に図1に関してこのようなGANについて簡単に説明する。

図1は複数のサービス網およびサービス網加入者に接続された典型的なGANの斜視図である。図1に示すGAN（10）はトランスポート網と相互接続され

たアクセス網を含んでいる。アクセス網は複数の基地局（例えば、BS1および

BS 2) を含んでいる。各基地局は各地理的エリア（例えば、いわゆるセル、C 1 および C 2）に対する通信カバレッジを提供する無線送信機および受信機を含んでいる。基地局は無線網コントローラ（RNC）12に接続されている。明示はしないが、ある基地局はRNC 12（例えば、BS 1 および BS 2）に接続することができ、別の基地局は1つ以上の他のRNCに接続することができる。複数のRNCを相互接続してその間に通信パスを提供することができる。

複数のサービス網（例えば、VOD網、PLMN、PSTN、インターネット）が各アクセス入力ポート（14, 16, 18, 20, 22, 24 および 26）を介してGAN 10のアクセス網に接続される。各サービス網はそれ自体の標準シグナリングプロトコルを使用してその内部シグナリングノード間で通信を行う。例えば、欧州中で実際に使用されているデジタルセルラーPLMNであるGlobal System for Mobile communication (GSM) はMultiple Application Part (MAP) シグナリングプロトコルを使用している。図1に示すように、アクセス網内のRNCは少なくとも1つのアクセス入力ポートを介してサービス網に接続されている。図からお判りのように、RNC 12はそれぞれアクセスポート20および24を介してPLMNおよびPSTNサービス網に接続されている。

GAN 10の無線カバレッジエリア内に移動端末28および30があつてアクセス網内の各基地局（例えば、BS 2）との接続を確立する。これらの移動端末は、例えば、セルラー電話機、移動無線電話機、恐らくはデジタルセルラー電話機に接続されたパソコン（ノートブック、ラップトップ、等）、もしくは移動テレビ受像機（VODに対する）とすることができる。移動端末と選択されたサービス網間の信号転送は特定の信号キャリアを介して行われる。例えば、信号はセルラー電話機（28）とPLMNサービス網との間を信号キャリアSC 1およびSC 2を介して転送される。

移動端末（例えば、28および30）はアクセス部およびサービス網部を含んでいる。移動端末のアクセス部はアクセス網の論理部であり、移動端末とRNC

12との間に信号キャリア（例えば、SC 2 および SC 4）を確立するのに必要

なシグナリングを処理する。移動端末のサービス網部はその端末のユーザが加入するサービス網の論理部である。移動端末のサービス網部は、その関連するサービス網の特定標準に従って、確立された信号キャリアSC1およびSC2（もしくはSC4）を介して信号を送受信する。信号キャリアSC2およびSC4（移動端末および基地局間）の無線インターフェイス部は時分割多元接続（TDMA）、符号分割多元接続（CDMA）、もしくは任意他種の多元接続インターフェイスとすることができる。

サービス網加入者はGANを介してその各サービス網へアクセスすることができる。GANは移動端末のサービス網部とそのサービス網との間で信号キャリア（例えば、SC1およびSC2）を介してメッセージをトランスペアレントに転送することができる信号キャリアインターフェイスを提供する。GANはそれに接続する全てのサービス網のシグナリングコネクションおよびトラフィックコネクションの特性を整合させてこの機能を達成する。したがって、GANは既存のサービス網のカバレッジを拡張しかつ加入者のモビリティを高めることができる。

GANの独特な特徴はそれ自体の加入者を持たないことである。GANのモバイルユーザはそれら自体のサービス網への永続的な加入者ではあるが、GANの一時的なユーザであるにすぎない。したがって、GANはこれらのユーザのアイデンティティを知らない（あるいは、知る必要がない）。しかしながら、移動端末とGANとの間の無線トラフィックを暗号化しようとする問題が生じる。

移動端末と基地局間の無線トラフィック（例えば、音声情報やデータ）は、通過される情報が秘密のままとされることを保証するために典型的に暗号化される。あるサービス網（例えば、GSM）はトラフィックを暗号化するが、他の大概のサービス網は暗号化しない。したがって、GANはその能力のないサービス網に対するトラフィックを暗号化できなければならない。しかしながら、GANはそのユーザ（サービス網加入者）のアイデンティティを知らないため、加入者端末のアイデンティティや認証を知らずに生成される暗号鍵を使用して無線トラフィックを暗号化できなければならない。残念ながら、既存の大概の移動無線網は認証パラメータを使用して暗号鍵を生成する暗号技術を使用している。言い換え

れ

ば、従来の移動通信網で無線トラフィックを暗号化するには、ユーザ端末のアイデンティティを知らなければならない。

発明の要約

ネットワークが端末のアイデンティティを知る必要なしに、移動端末と通信網間の通信を暗号化することが本発明の目的である。

ネットワークが各端末に対する個別の暗号鍵を維持する必要なしに、複数の移動端末と通信網間の通信を暗号化することも本発明の目的である。

端末が秘密暗号鍵を永続的に保存する必要なしに、移動端末と通信網間の通信を暗号化することが本発明のもう1つの目的である。

移動端末と通信網間の通信を暗号化しながら、呼開設時間を最小限に抑え、伝送遅延を最小限に抑え、かつデータスループットを最大限とすることが本発明のさらにもう1つの目的である。

本発明の1つの特徴に従って、ネットワークに関連する公開鍵を端末において保存し、端末において秘密鍵 (secret key) を生成し、端末において保存した公開鍵により秘密鍵を暗号化し、暗号化した秘密鍵を端末から送信し、暗号化した秘密鍵を端末において受信し、受信した暗号化した秘密鍵をプライベート鍵 (private key) により復号し、プライベート鍵は公開鍵に関連しており、後続トラフィックを秘密鍵により暗号化することにより通信網と通信端末間の通信を暗号化する方法が提供される。公開鍵が端末に保存されていない場合、端末は公開鍵の要求をネットワークへ送る。このようにして、ネットワークは端末との暗号化した通信を維持するために端末のアイデンティティを知る必要がない。

本発明のもう1つの特徴に従って、前記した目的およびその他の目的はネットワークから (非対称) 公開鍵をブロードキャストして通信網と通信端末間のトラフィックを暗号化する方法および装置により達成される。公開鍵は端末により受信される。ネットワークは公開鍵により暗号化した情報を復号するのに使用できるプライベート鍵を維持する。端末は自然発生乱数を秘密セッション (対称) 鍵と

して生成かつ保存し、対称セッション鍵を公開鍵により暗号化し、暗号化したセッション鍵をネットワークへ送る。ネットワークはプライベート鍵によりセッション鍵

を復号し、ネットワークおよび端末は共に後続通信を秘密セッション鍵により暗号化する。ここでも、通信網は端末との暗号化した通信を維持するために端末のアイデンティティを知る必要がない。

図面の簡単な説明

添付図と共に以下の詳細説明を読めば本発明の方法および装置をより完全に理解することができ、ここに、

図1は複数のサービス網およびサービス網加入者に接続された典型的な汎用アクセス網の斜視図。

図2は、本発明の好ましい実施例に従って、サービス網とサービス網加入者との間の無線トラフィックを暗号化する方法を実施することができる汎用アクセス網のトップレベル略ブロック図。

図3は図2に示すアクセス網の略ブロック図。

図4は、本発明の好ましい実施例に従って、汎用アクセス網と端末間の無線通信を暗号化するのに使用できる方法を示すシーケンス図。

図5は、本発明の好ましい実施例に従って、公開鍵の認証および鍵の所有者をデジタル署名により証明するのに使用できる方法のブロック図。

図面の詳細な説明

本発明の好ましい実施例およびその利点は図1－図5を見ればよく理解することができ、さまざまな図面において同様な対応する部品には同じ番号が付けられている。

本質的に、本発明の好ましい実施例に従って、移動端末は少なくとも1つの公開鍵をそれに関連する少なくとも1つのGANの一意的な識別キャラクタと共にメモリ位置に保存する。GANはそれに接続された全てのセルへその一意的な識別キャラクタをブロードキャストする。端末とそのGANとの間にコンタクトが開始されると、端末は受信した識別子を格納された識別子と比較し、一致すればランダム秘密鍵を生成し、そのGANの識別子に関連する公開鍵により秘密鍵を

暗号化し、暗号化した秘密鍵を送信する。GANは公開鍵に関連するプライベート鍵を使用して秘密鍵を復号する。その後秘密鍵は後続無線トラフィックを暗号化および復号するために端末およびGANにより使用される。GANは端末のアイデンティティを知ることなく端末との安全な通信を確保できることがお判りであろう。さらに、GANはこのような端末のアイデンティティを知る必要がないため、個別の端末暗号鍵のデータベースを維持する必要がない。さらに、端末は各通信セッションに対する新しい秘密鍵を生成できるため、それ自体の秘密鍵を保存する必要がない。

図2は、本発明の好ましい実施例に従って、サービス網とサービス網加入者間の無線トラフィックを暗号化する方法を実施することができる汎用アクセス網のトップレベル略ブロック図である。GAN100が図示されており、アクセス網104と相互接続されたトランスポート網102を含んでいる。複数のサービス網（例えば、PLMN, ISDN, PSTN, INTERNET, VOD）がそれぞれのアクセスポート（例えば、106, 108, 110, 112, 114）を介してトランスポート網102およびアクセス網104に接続されている。アクセス網104は複数のRNCおよび関連する基地局（例えば、RNC(1) - RNC(N)）を含んでいる。複数のRNCおよび関連する基地局は各無線インターフェイスにより複数の移動トランシーバ（端末）116, 118, 120および122に接続されている。各移動端末のユーザは少なくとも1つのサービス網PLMN等への加入者である。移動端末は図1に関して前記した方法でそれらの各サービス網と通信することができる。特に、RNCは端末とそれらの各サービス網間の通信を制御する。図2には複数の移動端末（116, 等）が図示されているが、それは単なる説明用にすぎない。1つ以上の固定無線端末もGAN100に接続することができ、したがって少なくとも1つのサービス網と通信することができる。

図3は図2に示すアクセス網104の略ブロック図である。アクセス網104は複数のRNC（例えば、RNC(1) - RNC(N)）を含んでいる。本実施例には複数のRNCが図示されているが、本発明は1つだけのRNCで実施する

ことができる。少なくとも1つのサービス網（例えば、130, 132, 134）が少なくとも1つの各アクセスポート（例えば、AP1, AP(N-1), AP(N)）を介して少なくとも1つのRNCに接続されている。少なくとも1つの基地局（例えば、BS(1), BS(N)）が各RNC（例えば、RNC

(1), RNC(N)）に接続されている。複数の基地局が図示されているが、本発明は1つだけの基地局で実施することができる。

移動端末（例えば、セルラー電話機118）が無線インターフェイスにより基地局BS(1)に接続されている。1台の端末(118)は単なる説明用であつてさらに1台以上の端末を図示できることが容易にお判りであろう。RNC（例えば、RNC(1)-RNC(N)）はその間の通信のために通信回線(136, 138)により相互接続されている。したがって、端末118はアクセス網104およびGAN100（図2）を介して任意のサービス網（例えば、130, 132, 134）との通信を確立することができる。アクセス網104のさまざまなアクセスポートへ切り替えることにより各サービス網に対して提供されるカバレッジを拡張できることがお判りであろう。すなわち、端末118はRNC(1)、相互接続回線136およびRNC(N-1)を介してサービス網132と通信することができる。あるいは、サービス網132がアクセスポートAP(1)に切り替えられると、端末118はRNC(1)を介してサービス網132と通信することができる。

図4は、本発明の好ましい実施例に従って、汎用アクセス網と端末間の無線通信を暗号化するのに使用できる方法を示すシーケンス図である。通信暗号化方法200はGANもしくは端末において開始することができる。例えば、本実施例では、ステップ204においてGAN（例えば、100）はそれに接続された全てのセル内の一意的な識別キャラクタを連続的にブロードキャストする。端末（例えば、118）はそのGAN部に配置された非揮発性メモリを含んでいる。端末は少なくとも1つの公開鍵を非揮発性メモリ内に保存している。各公開鍵と共に、端末は鍵の各期限、およびその鍵に関連する特定のGANを識別するGAN識別キャラクタも保存している。すなわち、端末のメモリ内に保存された各公開

鍵は特定のG A Nと関連づけられる。端末はG A Nに登録する（必ずしも呼を開設しない）ことによりコンタクトを開始する。端末内のプロセッサは受信したG A N識別子を保存された識別子と比較し、一致すれば（かつ、鍵の期限が切れていない）、プロセッサは識別されたG A Nに関連する保存された公開鍵を検索する。しかしながら、一致しなければ、端末はG A Nへ公開鍵送信要求を送る。

送信された公開鍵（および、その期限日付）は端末内に保存されて現在および後続通信セッション内の秘密鍵を暗号化するのに使用することができる。

ステップ206において、端末は（対称）秘密鍵を生成する（後述する）。ステップ208において、端末は検索した公開鍵を使用して秘密鍵を暗号化する。ステップ210において、端末は暗号化した秘密鍵を識別されたG A Nへ送る。ステップ212において、G A Nは秘密鍵を復号し、それはステップ214において後続通信セッション中にトラフィックを暗号化するためにG A Nおよび端末により使用される（後述）。

あるいは、G A Nとのセッションの終わりに、端末はそのセッションに使用した公開鍵を保存する。端末もしくはG A Nが新しい通信セッションを開始すると、端末はG A Nとの最終セッションから保存された公開鍵を検索し、その公開鍵を使用して後続セッションに使用される秘密鍵を暗号化する。その保存された公開鍵の使用が不成功である場合には、端末はG A Nへ新しい公開鍵要求を送る。ネットワークチャネルは公開鍵の送信に占有されないため、この技術によりネットワークスループットが有利に増大する。しかしながら、特定のG A Nとの過去のセッションから公開鍵が保存されていない場合には、端末はまだG A Nへ要求して公開鍵を受信することができ、それを使用して後続セッションに使用される秘密鍵を暗号化することができる。いずれにせよ、比較的大きい（ビットワイズ：b i t - w i s e）公開鍵をG A Nから送信するのではなく端末内に保存することにより、無線伝送遅延を著しく低減し、相当な量のネットワーク伝送時間を節減し、データスループットを増大することができる。

図4には、本発明のもう1つの実施例に従って、汎用アクセス網と移動端末間の無線通信を暗号化するのに使用できる方法も図示されている。例えば、サービ

ス網と端末（例えば、PLMNと端末118）間で通信したい場合には、サービス網もしくは端末が呼開設メッセージとの通信を開始することができる。ステップ202において、GANと端末間の初期接続が確立されると、サービス網は後続トラフィックが暗号化されることを要求することができる。そうであれば、ステップ204において、まだ初期呼開設プロセス中に端末は1つ以上の基地局（例えば、BS（1）-BS（N））から連続的にブロードキャストされる公開

鍵を受信する。

本実施例では、全てのRNCが少なくとも1つの公開鍵／プライベート鍵対（各RNC内の同じ対）をメモリ記憶位置に維持することができる。GANによりブロードキャストされた公開鍵はそのGANとのコンタクトを開始した端末（118）により受信される。好ましくは、呼開設手順および公開鍵転送手順は共にRNCにより実施され、それはアクセスポートを介して当該サービス網（例えば、RNC（1）からAP（1）からPLMN130）に接続されている。あるいは、基地局（例えば、BS1）は公開／プライベート鍵対を維持して公開鍵を端末へブロードキャストその他で転送するように構成することができる。

RNCはそのカバレッジエリア内の全てのセル内に公開鍵をブロードキャストすることができる。したがって、GANは端末にGANから鍵を要求させるのではなく公開鍵をブロードキャストするため、端末はより高速にGANに登録することができ、かなり短時間内で呼を開設することができる。あるいは、複数のセル内に公開鍵をブロードキャストする代わりに、RNCは端末とのコンタクトを確立している基地局を介して直接公開鍵を転送することができる。しかしながら、呼開設の前に複数のセル内へ公開鍵をブロードキャストする方法により、GANの専用トラフィックチャネルのロードを有利に減少することができる。

全ての実施例に対して、端末がGANに登録されるかぎり、同じ鍵がGANおよび端末に保存されるため、そのGANとの全ての後続通信に同じ公開鍵を使用することができる。あるいは、所定の方式やアルゴリズムに従って、もしくはGANオペレータの思いつきで、公開鍵を周期的に変えることができる。オペレータが公開鍵を周期的に変えたい場合には、各公開鍵の期限日付を端末に格納する

とそれに関したそれらの使用が容易になる。さらに、好ましい実施例では、公開鍵が変えられると、所定期間G A Nによりブロードキャストされて、端末の新しい公開鍵に対する要求数を最小限に抑えることができる。

前記したように、ステップ202において、G A Nは1つ以上の非対称公開鍵／プライベート鍵対を維持することができる。その場合、いわゆる“R S A アルゴリズム”を使用して公開鍵／プライベート鍵対を生成することができる。R S A アルゴリズムは素数の因数分解の困難さと大きい素数を発生する（確率アルゴリズムを使用して）容易さとを組み合わせる暗号鍵を公開部および非公開部へ分離する。

特に、文字PおよびQが素数を表し、文字Mが非暗号化メッセージを表し、文字CがMの暗号化形式を表すものとする、R S A アルゴリズムは次式で表すことができる。

$$M^E \bmod PQ = C \quad (\text{暗号化メッセージ} M) \quad (1)$$

$$C^D \bmod PQ = M \quad (\text{復号メッセージ} C) \quad (2)$$

ここに、 $(DE - 1)$ 項は $(P - 1)(Q - 1)$ の倍数である。本実施例では、指数Eは3に設定される。公開およびプライベート鍵は各々が2つの数字で構成されている。例えば、 (PQ, D) で表される数字がプライベート鍵を構成し、 (PQ, E) で表される数字が公開鍵を構成する。Eに対する同じ値が一貫して使用されるため、数字のPQ部だけを要求に応じて送出するもしくはブロードキャストして公開鍵に使用することができる（例えば、ステップ204において）。プライベート鍵を知ることにより、公開鍵で暗号化されたいかなるメッセージも復号することができる。

図4に戻って、ステップ206において、端末(118)は非対称公開鍵を受信および／もしくは保存する。端末はランダム対称秘密鍵を生成する。通信を完全なセッションに対して好ましく暗号化するのに使用されるランダム秘密鍵は4つの方法の中の少なくとも1つの方法で生成することができる。1つの方法を使用して、端末は受信信号の強度測定値からいくつかのサンプルを取り出し、その下位ビットを接続し、結果を処理して乱数を作り出す。受信信号の下位ビットは十

分そのノイズレベル内にあるため、自然に生じる真の乱数が発生される。第2の乱数発生方法はマイクロホンに接続されたA/Dコンバータの入力に生成されるランダムノイズ信号を使用することである。ここでも、この方法を使用して、秘密鍵に対して自然に生じる真の乱数を発生することができる。第3の乱数発生方法は端末に対して受信信号の位相測定値からサンプルを採り、その下位ビットを接続し、結果を処理して乱数を作り出すことである。第4の乱数発生方法は端末に対して音声コーデックの符号化部からサンプルを採り、その下位ビットを接続し、結果を処理して乱数を作り出すことである。

あるいは、端末において発生された乱数を擬似乱数発生器用シードとして使用することができる。シードはGANからの公開鍵により暗号化され、GANへ送られる。シードはGANおよび端末内で同時に使用されて擬似乱数を発生する。このように発生される擬似乱数をGANおよび端末が後続通信セッションのための秘密鍵として使用することができる。

セッション鍵は擬似乱数列内の異なる数字へ周期的に変えることができる。例えば、セッション鍵は所定量のデータが暗号化された後やトラフィックが所定量の時間暗号化された後等の、いくつかの理由に対して変えることができる。端末もしくはGANは秘密鍵の変化を開始することができ、あるいは所定の方式やアルゴリズムに従って鍵を変えることができる。例えば、秘密セッション鍵を変える要求は“セッション鍵変化要求”メッセージを送るか、あるいは送られたメッセージのヘッダー内に“セッション鍵変化要求”ビットを設定して実施することができる。

さらに、前記した擬似乱数発生方法により、より短いセッション鍵を生成しより複雑ではない暗号化アルゴリズムを使用することができる。したがって、GAN特に端末において相当な量の処理能力を節減することができる。セキュリティと計算要求との間のトレードオフを行うために、端末は使用されるセッション鍵の長さを選択するように構成することができる。例えば、端末のプロセッサはその長さでセッション鍵を生成するか、あるいは擬似乱数発生器の出力から使用されるビット数を指定することにより秘密セッション鍵の長さを選択することができる。あるいは、端末は擬似乱数発生器の出力範囲を指定して所定長を設定することが

きる。

別の方法を使用して秘密セッション鍵に対する擬似乱数を発生することができる。例えば、“遅延フィボナッチ” (L a g g e d F i b o n a c c i) 型の擬似乱数発生器を使用して、擬似乱数列内の第 n 番数字 N_n を次のように計算することができる。

$$N_n = (N_{n-k} - N_{n-1}) \bmod M \quad (3)$$

ここに、 k および 1 はいわゆる遅延であり、 M は発生される擬似乱数の範囲を規定する。最適結果に対して、最大遅延は 1000 と 10000 の間でなければならない。比較的長い鍵が望まれる場合には、式3により作り出された複数の擬似

乱数を接続してより長い鍵を作り出すことができる。式3により作り出された擬似乱数が 0 と 1 との間の浮動小数点数字である場合には、 M を 1 に設定することができる。このような浮動小数点擬似乱数のビットパターンは対称暗号鍵として使用することができる。

秘密セッション鍵を生成するのに使用できるもう1つの擬似乱数発生器は 0 と 1 との間に均一に分布された擬似乱数を作り出すアルゴリズムに基づいている。特に、擬似乱数 N_n のシード X_0 、 Y_0 および Z_0 は 1 と 30000 との間の整数値に初期設定される。次に、擬似乱数は次のように計算される。

$$X_n = 171 * (X_{n-1} \bmod 177) - (2 * X_{n-1} / 177) \quad (4)$$

$$Y_n = 172 * (Y_{n-1} \bmod 176) - (35 * Y_{n-1} / 176) \quad (5)$$

$$Z_n = 170 * (Z_{n-1} \bmod 178) - (63 * Z_{n-1} / 178) \quad (6)$$

X_n 、 Y_n および Z_n のいずれの値も、それぞれ、ゼロよりも小さい場合には、 X_n は $X_n + 30269$ に等しく設定され、 Y_n は $Y_n + 30307$ に等しく設定され、あるいは Z_n が $Z_n + 30323$ に等しく設定される。擬似乱数 N_n は $((X_n / 30269 + Y_n / 30307 + Z_n / 30323) \bmod 1)$ に等しくなり、 X_n 、 Y_n および Z_n は浮動小数点数字であり、“ \bmod ” はこれらの数字を因数分解できることを意味する。このアルゴリズムにより発生される浮動小数点数字は対称暗号鍵として使用するのに適したビットパターンを形成する。このような鍵の長さは発生された複数の擬似乱数を接続して延長することができる。

図4に示す方法に戻って、ステップ208において、好ましくは前記したRSAアルゴリズムを使用して端末は秘密対称鍵を公開鍵により暗号化する。例えば、端末において生成された秘密対称鍵は文字SKで表されるものとする。RSAアルゴリズムの式1を使用して、秘密鍵は次のように暗号化される。

$$M^E \text{ mod } PQ = C$$

ここに、(PQ, E)は公開鍵を表し、MはSKに等しく、CはSKの暗号化バージョンである。指数Eは3に等しい。

好ましい実施例では、端末は暗号化した秘密鍵をメッセージフォーマット化し、それにはヘッダーおよびメッセージフィールドが含まれる。ヘッダーはメッセージフィールド内で後に続く暗号化した秘密鍵に関連する制御情報を提供する。
へ

ッダー内の1ビットはヘッダーに続くメッセージフィールドが暗号化されることを表示するように設定することができる。すなわち、メッセージの秘密鍵フィールドしか暗号化されない。メッセージのヘッダーは普通文で送られる。したがって、ヘッダーは後続メッセージフィールドが暗号化されるかどうかを表示し、暗号化される場合にはメッセージのその部分しか復号されないため、RNCにおいて相当な量のネットワーク処理時間を節減することができる。

ステップ210において、端末(118)は暗号化した秘密鍵(C)をコンタクトした基地局(例えば、BS(1))を介してGANへ送る。好ましい実施例では、この秘密鍵は後続通信のために使用される。あるいは、後続通信セッション中の任意の時間に、端末は新しい秘密鍵を生成し、それを公開鍵により暗号化し、新しい暗号化した秘密鍵をGANへ送ることができる。特定の秘密鍵がセッションのために使用される時間量を低減することにより、秘密鍵が許可されないユーザにより壊される尤度も低減されるため、セッションのセキュリティが高められる。
。

ステップ212において、RNC(例えば、RNC(1))は基地局から暗号化した秘密鍵(C)を受信し、RSAアルゴリズムのプライベート鍵部を使用して秘密鍵を復号する。例えば、RSAアルゴリズムの式2(前記)を使用して、

受信した暗号化した秘密鍵 (C) は次のように復号される。

$$C^D \bmod PQ = M$$

ここに、(PQ, D) はプライベート鍵を表し、MはSK (秘密鍵) に等しい。

ステップ214において、RNCと端末間の後続無線トラフィックが秘密鍵により暗号化および復号され、それはRNCと端末の両方にとって現在既知である。既知の対称暗号化アルゴリズムを使用して、例えば、1、2もしくは3パス Data Encryption Standard (DES) アルゴリズム、もしくはFast Encipherment Algorithm (FEAL) 等の秘密鍵により後続無線トラフィックを暗号化および復号することができる。

さらにもう1つの暗号化として、RSAアルゴリズムを使用して公開／プライベート鍵対を生成する替わりに、いわゆるディフィーヘルマン“指数鍵交換”アルゴリズムを使用して端末およびGANに秘密セッション鍵を承諾させることがで

きる。この暗号化方式を使用する時は、2つの数字 (α , q) がGANにおいて保存される。通信セッションの開始時に、RNCは2つの数字を直接端末へ送る (もしくは、数字をブロードキャストする)。数字 α および q は次の基準に合致する必要がある。 q は (ガロア) 有限体 $GF(q) = 1, 2, \dots, q-1$ を定義する大きい素数であり、 α は $GF(q)$ の固定原始元 (primitive element) である。すなわち、($\alpha^x \bmod q$) の指数 (x) は $GF(q)$ の全ての元 $1, 2, \dots, q-1$ を作り出す。秘密セッション鍵の承諾を発生するために、2つの数字 (α , q) はGANから端末へ直接へ送られる (もしくは、ブロードキャストされる)。あるいは、2つの数字は端末の非揮発性メモリ内に既に常駐することができる。端末 (118) は乱数 X_T ($1 < X_T < q-1$) を発生し、 $Y_T = \alpha^{X_T} \bmod q$ の値を計算する。GAN (例えば、RNCもしくは基地局) は乱数 X_G ($1 < X_G < q-1$) を発生し、 $Y_G = \alpha^{X_G} \bmod q$ の値を計算する。乱数は自然発生、真の乱数発生に関して前記した方法を使用して端末において発生することができる。

Y_T および Y_G は暗号化されずに各GANおよび端末へ転送される。数字 Y_G を

受信すると、端末は $K_s = Y_c^{x_r} \bmod q = \alpha^{x_c x_r} \bmod q$ の値を計算する。数 Y_r を受信すると、G A N は $K_s = Y_r^{x_c} \bmod q = \alpha^{x_r x_c} \bmod q$ の値を計算する。 X_r の数字は端末において秘密のままとされ、 X_c の数字はG A Nにおいて秘密のままとされるが、 K_s の値は今や端末およびG A Nの両方で既知である。したがって、 K_s の数字は両者により通信セッション暗号鍵として使用される。許可されないユーザは X_r もしくは X_c のいずれかを知らず Y_r および Y_c から鍵 K_s を計算しなければならず、それは手に負えない計算過程である。指数鍵交換アルゴリズムを使用することの著しいセキュリティ上の利点は、G A Nが秘密プライベート鍵データを永久ベースで維持する必要がないことである。

要約すれば、通信セッションが最初にG A Nと端末との間で開始されると、端末はG A Nにより連続的にブロードキャストされ、端末の内部メモリから検索され、あるいはG A Nから要求されている非対称公開鍵を受信する。G A Nは公開鍵により暗号化された情報を復号するのに使用できるプライベート鍵を維持する。端末は自然発生乱数を秘密セッション（対称）鍵として生成して保存し、対称セシヨ

ン鍵を公開鍵により暗号化し、暗号化したセッション鍵をG A Nへ送る。G A Nはセッション鍵をプライベート鍵により復号し、G A Nおよび端末の両方が後続通信を秘密セッション鍵により暗号化する。通信開始時にG A Nから端末へ公開鍵を転送することの主要な技術的利点は、G A Nが端末との通信を暗号化させるのに端末のアイデンティティを知る必要がないことである。しかしながら、許可されないユーザがG A Nを装って端末へ公開鍵を送ろうとすると問題が生じる。その場合には、後述するように、端末は受信した公開鍵およびG A Nのアイデンティティを認証するように構成することができる。

例えば、G A Nから端末へ公開鍵が転送される時は、鍵は公開鍵“証明書”により転送することができる。この証明書は関連する公開鍵およびその所有者が本物であるという証拠となる。“信頼された”サードパーティが公開鍵を証明書と一緒に発行することができ、それにはサードパーティのアイデンティティおよび公開鍵を認証する“デジタル署名”が含まれている。証明書は、また、G A Nの

アイデンティティおよび証明書に期限がある場合にはそれも含むことができる。

本発明の1つの局面において、GANは証明書および公開鍵を端末へ送る。その場合、サードパーティの公開鍵は加入端末に予め保存される（先験的）。

図5は、本発明に従って、公開鍵およびその所有者の認証をデジタル署名により証明するのに使用することができる方法のブロック図である。公開鍵証明書にデジタル署名してその認証を検証する方法（300）はステップ302で開始される。ステップ302において、端末へ転送される公開鍵の所有者に関する暗号化されていない情報を含む“証明書”が信頼されたサードパーティにより準備される。暗号化されていない情報には公開鍵および証明書の期限も含まれる。ステップ304において、“未署名”証明書が取消し不可アルゴリズム（例えば、ハッシングアルゴリズム）により処理されステップ306においてメッセージダイジェストが作り出され、それは証明書上に含まれる情報のダイジェストすなわち短縮バージョンである。ステップ308において、ダイジェスト情報は異なる公開／プライベート鍵対のプライベート鍵により暗号化される。好ましくは、前記式1および式2と同様なRSAアルゴリズムを使用してこの鍵対が導出される。したがって、ステップ310において、元の暗号化されていない情報（通信セシ

ョンに使用される公開鍵を含む）および、証明書発行者のプライベート鍵により現在暗号化されているダイジェスト情報を含むデジタル署名済み公開鍵証明書が作り出される。次に、デジタル署名済み公開鍵証明書はGANとのコンタクトを開始している端末へ転送される。

ステップ312において、デジタル署名済み証明書を受信すると、端末のプロセッサはドキュメントの暗号化されていない部分および暗号化された部分を解析する。ステップ314において、暗号化されていない情報はステップ304で使用したハッシングアルゴリズムと同じアルゴリズムを使用して処理される。ステップ316において、暗号化されていない情報の第2のダイジェストバージョンが端末において作り出される。ステップ318において、端末のプロセッサは予め保存された証明書発行者の公開鍵をメモリから検索し、RSAアルゴリズムを使用して証明書からの暗号化されたダイジェスト情報を復号する。したがって、

ステップ320において、暗号化されていないダイジェストされた情報のもう1つのバージョンが作り出される。ステップ322において、端末は暗号化されていないダイジェストされた情報の2つのバージョンを比較し、比較した情報が同じであれば証明書の署名およびセッション公開鍵は本物と推定される。証明された公開鍵は端末が秘密セッション鍵を暗号化するのに使用することができる。

本発明の方法および装置の好ましい実施例を添付図に示し前記詳細な説明で説明してきたが、本発明は開示した実施例に限定されるものではなく、請求の範囲に明記された発明の精神を逸脱することなくさまざまな再構成、修正および置換が可能である。

【図1】

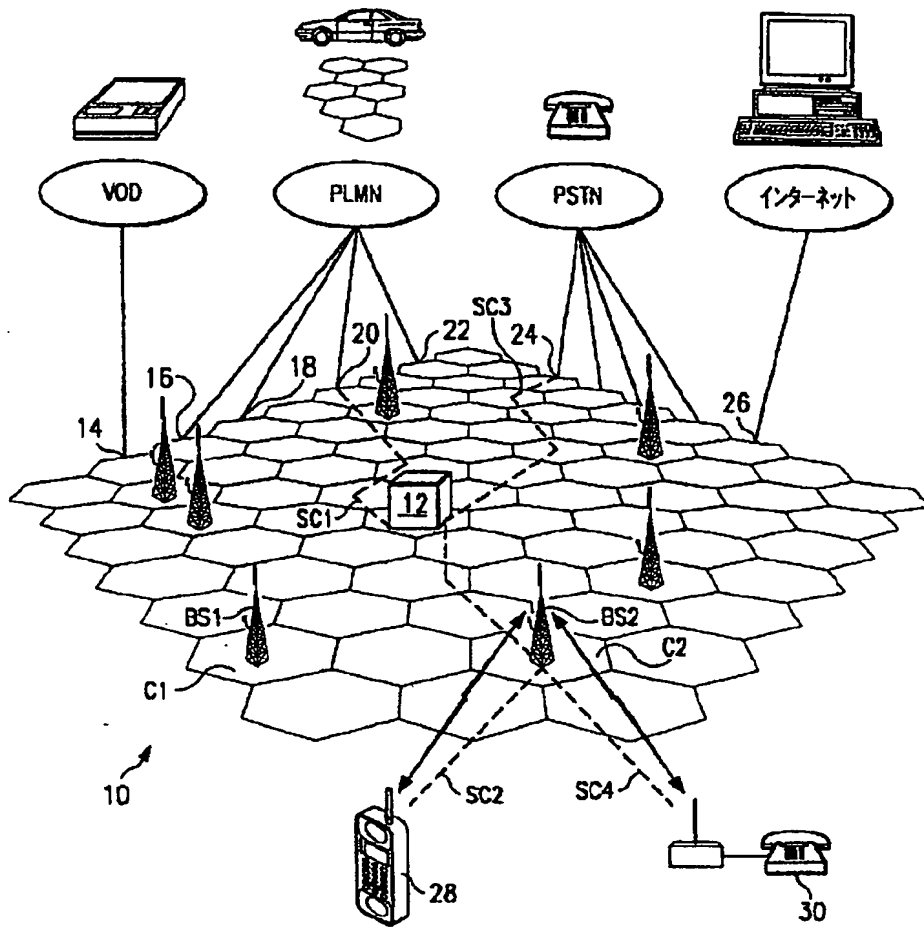


FIG. 1

【図 2】

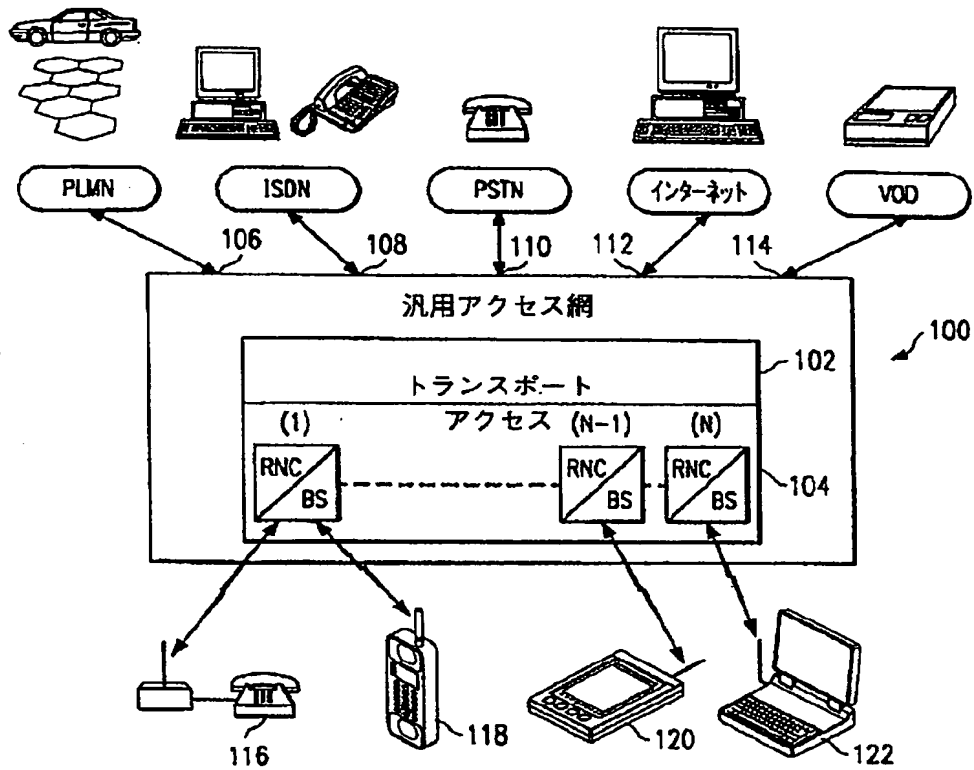


FIG. 2

【図 3】

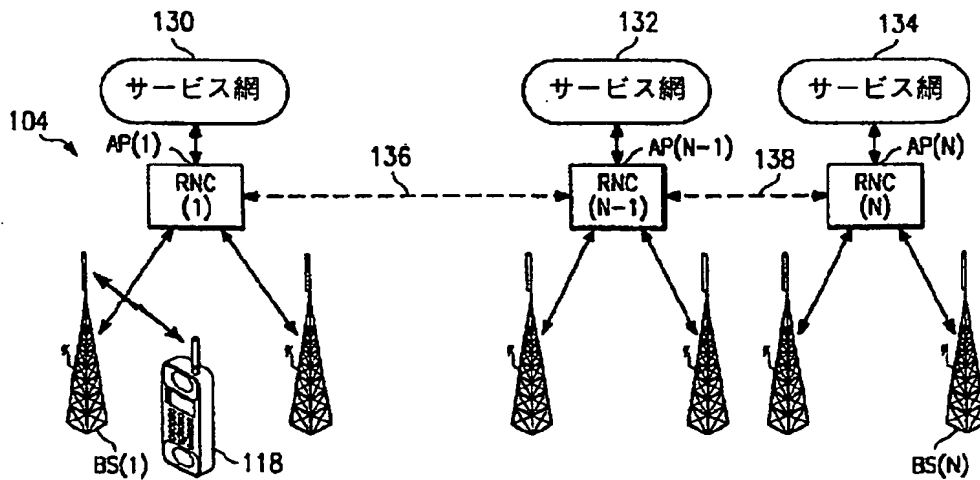
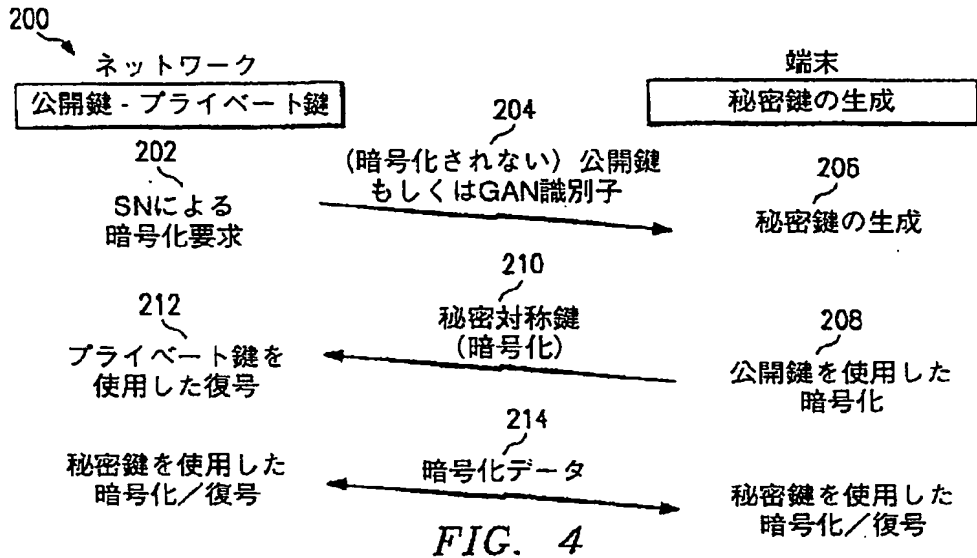
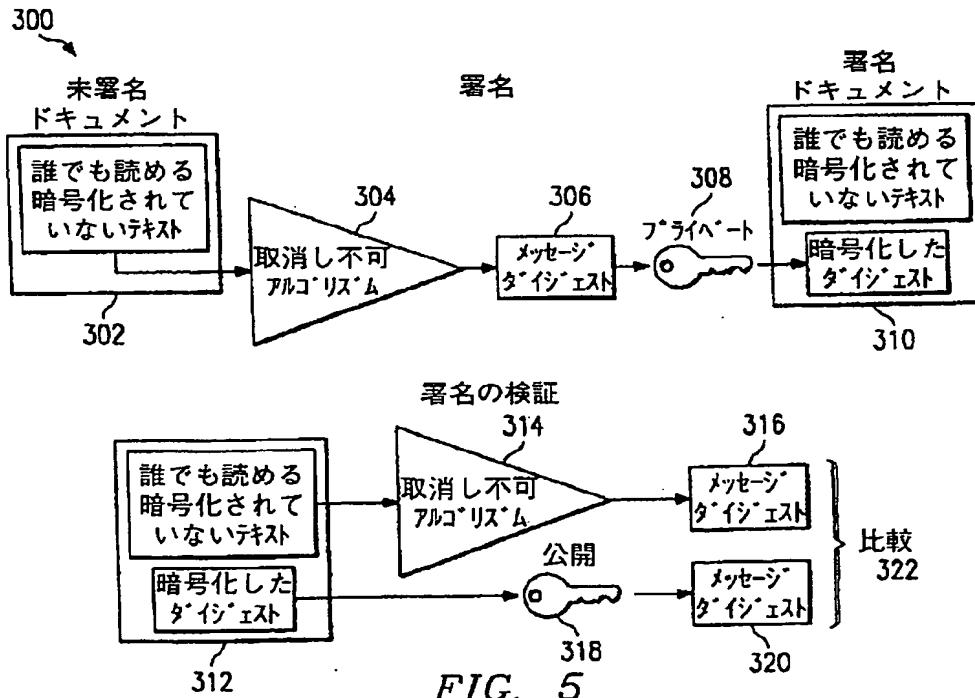


FIG. 3

【図4】



【図5】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 97/01407

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 H04L9/08 H04Q7/32		
According to International Patent Classification(IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 H04L H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 222 140 A (BELLER ET AL.) 22 June 1993 see column 4, line 57 - column 5, line 3 see column 5, line 13 - line 37	1,2,7, 10,28, 29,34, 42-44
A	GB 2 297 016 A (KOKUSAI DENSHIN DENWA) 17 July 1996 see page 19, line 11 - page 21, line 2; figure 7	28,44
-/--		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		
<input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "A" document member of the same patent family		
Date of the actual completion of the international search		Date of mailing of the international search report
19 November 1997		02/12/1997
Name and mailing address of the ISA European Patent Office, P.O. Box 5818 Patentplan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 21 851 opo nl Fac. (+31-70) 340-3016		Authorized officer Holper, G

INTERNATIONAL SEARCH REPORT

International Application No

PCT/SE 97/01407

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MEVEL F ET AL: "Distributed communication services in the Masix system" CONFERENCE PROCEEDINGS OF THE 1996 IEEE FIFTEENTH ANNUAL INTERNATIONAL PHOENIX CONFERENCE ON COMPUTERS AND COMMUNICATIONS (CAT. NO.96CH35917), CONFERENCE PROCEEDINGS OF THE 1996 IEEE FIFTEENTH ANNUAL INTERNATIONAL PHOENIX CONFERENCE ON COMPUTERS AND, ISBN 0-7803-3255-5, 1996, NEW YORK, NY, USA, IEEE, USA, pages 172-178, XP000594787 see page 174, right-hand column, line 25 - line 29 see page 176, right-hand column, line 26 - page 177, left-hand column, last line; figure 5 -----	28,43,44
A	PATENT ABSTRACTS OF JAPAN vol. 95, no. 008 & JP 07 203540 A (N T T IDOU TSUUSHINMOU KK), 4 August 1995, see abstract -----	1,34
A	EP 0 067 977 A (SIEMENS) 29 December 1982 see abstract; figure 2 -----	24

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 97/01407

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5222140 A	22-06-93	NONE	
GB 2297016 A	17-07-96	JP 8195741 A	30-07-96
EP 67977 A	29-12-82	DE 3123167 C	24-02-83

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, YU

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☒ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☒ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.